NCSC-9

NATIONAL COMMUNICATIONS SECURITY (COMSEC) GLOSSARY

1 SEPTEMBER 1982

NATIONAL COMMUNICATIONS SECURITY COMMITTEE

FOR OFFICIAL USE ONLY

NCSC
NATIONAL
COMMUNICATIONS
SECURITY
COMMITTEE

SEPTEMBER 1982

FOREWORD

This Glosssary was developed under a provision of the National Communications Security Directive, dated 20 June 1979, which requires the NCSC to issue a glossary "containing definitions unique to communications security." It is the standard and authoritative reference for specific meanings of U.S. communications security (COMSEC) terms and takes precedence over all other glossaries and dictionaries with respect to the COMSEC use of the definitions for the terms contained in it. To keep this Glossary unclassified, certain sensitive COMSEC terms have been omitted. A classified document containing definitions of TEMPEST terms prepared by the Subcommittee on Compromising Emanations (SCOCE) was issued as NCSC-3, dated 30 March 1981.

This Glossary is effective upon receipt and, together with the TEMPEST Glossary, supersedes the "Glossary of Communications Security and Emanations Security Terms," dated October 1974 (USCSB 2-17), which should be destroyed.

Use of this Glossary should be restricted to official activities of U.S. Government organizations, and reasonable care should be taken to keep it in official channels. However, it is permissible to issue this publication to U.S. commercial companies under contract to the U.S. Government on COMSEC-related activities. Although individual terms in the basic Glossary are unclassified, reproduction in any form should bear the caveat, "For Official Use Only." Individual terms or definitions may be used without restriction.

This Glossary is published for government-wide use and as a reference for specific definitions of the technical terms most frequently used in the field of COMSEC. If this document is to be useful to all departments and agencies, it must be kept up-to-date to reflect definitions, and suggestions for new terms to be included in subsequent revisions are encouraged, and should be addressed to:

Executive Secretary, NCSC
Room C2A40, Ops Bldg #3
National Security Agency
Ft. George G. Meade, MD 20755

Responsibility for distributing this Glossary to their subordinate elements rests with the chiefs of the Military Services and the heads of the Federal Departments and Agencies. These officials may request additional copies, as required, from the Executive Secretary, NCSC.

Donald C. Latham
DONALD C. LATHAM
Chairman

NATIONAL COMMUNICATIONS SECURITY (COMSEC) GLOSSARY

A

accounting legend code (ALC) — A numeric code used within the COMSEC Material Control System to indicate the minimum accounting controls required for items of TSEC-nomenclatured COMSEC material. ALC categories are specified in NACSI 4005.

advanced development model (ADM) — A model of a complete COMSEC equipment for experimentation or tests intended to demonstrate the technical feasibility of the design and the ability to meet existing performance requirements; also to provide engineering data for further development.

assembly — A group of parts, elements, subassemblies, and circuits assembled as a separately removable item of a COMSEC equipment.

authentication — Measures designed to provide protection against fraudulent transmission and imitative communications deception by establishing the validity of a transmission, message, station, or individual.

authentication system — A cryptosystem or a cryptographic process used for authentication.

authenticator — A symbol or group of symbols, or a series of bits, selected or derived in a prearranged manner and usually inserted at a predetermined point within a message or transmission for the purpose of attesting to the validity of the message or transmission.

auto-manual cryptosystem — A cryptosystem in which a programmable hand-held device is used to perform encoding and decoding functions.

B

BLACK bulk facility — A telecommunications facility which employs crypto-equipment to protect multichannel trunks passing encrypted or unclassified information.

BLACK designation — A designation applied to all telecommunications circuits, components, equipment, and systems which handle only encrypted or unclassified signals; and to telecommunications areas in which no classified signals occur.

bogus message — A message sent for some purpose other than its content, and which may consist of dummy groups or meaningless text.

brevity code/brevity list — A code which has the sole purpose of shortening messages rather than the concealment of their content.

bulk encryption — Encryption of all channels of a multi-channel telecommunications trunk.

C

call sign — The symbol used to identify a member of a communications net.

callsign cipher — A cryptosystem used to encipher or decipher call signs, address groups, or address indicating groups.

canister — A type of protective package used for cryptovariables in tape form which are designated "CRYPTO."

card reader insert board (CRIB) — A removable component of certain machine cryptosystems which is installed in place of the card reader circuit plate in order to alter the cryptovariable provided by the key card.

central office of record (COR) — The activity within a department or agency charged with responsibility for maintaining records of accountability of all accountable COMSEC material received by or generated within the department or agency.

challenge and reply authentication — A prearranged procedure whereby one communicator requests authentication of another communicator and the latter establishes his validity by a proper reply.

check decryption — In off-line cryptographic operation, the process of insuring by decryption (before transmission) that a message is properly encrypted.

check word — A group of characters or bits used to verify that the cryptovariable has been properly filled into a cryptographic equipment.

cipher group — A group of letters or numbers (usually five in number) used in encrypted versions of messages, protected by off-line manual and machine cryptosystems to facilitate transmission or encryption/decryption.

cipher system — A cryptosystem in which the cryptographic treatment is applied to plain text elements of equal length.

cipher text — Enciphered information.

cipher text auto-key (CTAK) — A cryptographic logic which uses previous cipher text to produce key.

ciphony — The process of enciphering digitized audio signals.

code — Any system of communication in which arbitrary groups of letters, numbers, or symbols represent units of plain text of varying length. Coding has three distinctly different applications:

1. In the broadest sense, coding is a means of converting information into a form suitable for communications or encryption; e.g., coded speech, Morse code, teletypewriter codes, etc. No security is provided.
2. Brevity lists are codes which are used to reduce the length of time necessary to transmit information; e.g., long, stereotyped sentences may be reduced to a few characters which are transmitted. No security is provided.
3. A cryptosystem in which the cryptographic equivalents (usually called code groups) typically consisting of letters or digits (or both) in otherwise meaningless combinations are substituted for plain text information elements which are primarily words, phrases, or sentences. Security is provided.

code book — 1. A book or other document containing plain and code equivalents systematically arranged.
2. A technique of machine encryption employing word substitution.

code group — A group of letters or numbers, or both, assigned in a code system to represent a plaintext element which may be a word, phrase or sentence.

code vocabulary — The set of plaintext items to which code equivalents are to be assigned in a code system.

cognizant agent — See hostile cognizant agent

common fill devices — A family of devices developed to read in, transfer and store keying variables. Included are the KYK-13/TSEC Electronic Transfer Device, the KYX-15/TSEC Net Control Device and the KOI-18/TSEC General Purpose Tape Reader.

communications cover — The technique of concealing or altering the characteristics of communications patterns for the purpose of denying an enemy information that would be of value.

communications deception — The deliberate transmission, retransmission, or alteration of communications in a manner intended to cause a misleading interpretation of these communications.

communications privacy — The protection afforded to information transmitted in a secure telecommunications system or network to conceal it from persons within the system or network.

communications profile — An analytic model of the communications associated with an organization or activity as they might appear to a hostile SIGINT organization; the model results from a systematic examination of applied COMSEC measures, communications content and patterns, and the functions they reflect.

communications protection — Applying communications security (COMSEC) measures to telecommunications in order to deny unauthorized persons unclassified information of value, to prevent disruption, or to ensure the authenticity of such telecommunications.

communications security (COMSEC) — Protective measure taken to deny unauthorized persons information derived from telecommunications of the United States Government related to national security and to ensure the authenticity of such communications. Such protection results from the application of security measures (including cryptosecurity, transmission security, and emissions security) to electrical systems generating, handling, processing, or using national security or national security-related information. It also includes the application of physical security measures to communications security information or materials.

compromise	The known or suspected exposure of clandestine personnel, installations or other assets, or of classified information or material, to an unauthorized person.
compromising emanations	Unintentional intelligence-bearing signals which, if intercepted and analyzed, disclose national security information transmitted, received, handled or otherwise processed by any information-processing system.
computer cryptography	The use of a crypto-algorithm in a computer, microprocessor or micro-computer to perform encryption/decryption to protect information or to authenticate users, sources or information.
computer security	The protection resulting from all measures designed to prevent deliberate or inadvertent unauthorized disclosure, acquisition, manipulation, modification, or loss of information contained in a computer system, as well as measures designed to prevent denial of authorized use of the system.
COMSEC	The abbreviation for Communications Security.
COMSEC account	An administrative entity, identified by an account number, responsible for maintaining custody and control of COMSEC material.
COMSEC aids	All COMSEC material, other than equipments or devices, that perform or assist in the performance of cryptographic functions or relate to associated functions and equipments, and are required in the production, operation, and maintenance of cryptosystems and components thereof. Some examples are: COMSEC keying material, callsign/frequency systems, and supporting documentation, such as operating and maintenance manuals.
COMSEC assessment	A determination of the relative significance of telecommunications vulnerabilities and the threats thereto.
COMSEC control program	A set of instructions or routines for a computer which controls or affects externally performed functions of key generation, cryptovariable generation and distribution, message encryption/decryption, or authentication.
COMSEC custodian	The individual designated by proper authority to be responsible for the receipt, transfer, accountability, safeguarding, and destruction of COMSEC material issued to a COMSEC account.

COMSEC end item	A part or combination of component parts and/or material which is ready for its intended use in a COMSEC application.
COMSEC equipment	Equipment designed to provide security to telecommunications by converting information to a form unintelligible to an unauthorized interceptor and by reconverting such information to its original form for authorized recipients, as well as equipment designed specifically to aid in, or as an essential element of the conversion process. COMSEC equipment is crypto-equipment, crypto-ancillary equipment, cryptoproduction equipment, and authentication equipment.
COMSEC evaluation	An assessment of the effectiveness of the COMSEC measures applied to a particular telecommunications system and of the need, if any, for the application of additional COMSEC measures.
COMSEC facility	A facility which contains classified COMSEC material.
COMSEC firmware	Program information contained in a Programmable Read-Only Memory (PROM), Read-Only Memory (ROM), or similar device incorporating a COMSEC function.
COMSEC information	All information concerning COMSEC and all COMSEC material.
COMSEC insecurity	Any occurrence which jeopardizes the security of COMSEC material or the secure electrical transmission of national security or national security-related information.
COMSEC material	COMSEC aids, equipments and components thereof, and devices which are identifiable by the Telecommunications Security (TSEC) nomenclature system or a similar system of a U.S. department or agency, foreign government, or international organization.
COMSEC material control system (CMCS)	The logistic system through which accountable COMSEC material is distributed, controlled and safeguarded. It consists of all COMSEC Central Offices of Record, cryptologistic depots and COMSEC accounts/ subaccounts.
COMSEC measures	All cryptographic, transmission security, emission security, and physical security techniques employed to protect telecommunications.

COMSEC monitoring

The act of listening to, copying or recording transmissions of one's own official telecommunications to provide material for analysis in order to determine the degree of security being provided to those transmissions. It is one of the techniques of COMSEC Surveillance.

COMSEC profile

An identification of all COMSEC measures and materials available for a given operation, system, or organization, and a determination of the amount and type of use of those measures and materials.

COMSEC signals acquisition and analysis

The acquisition of radio frequency propagation and its subsequent analysis to determine empirically the vulnerability of the transmission media to interception by foreign intelligence services. This process includes cataloging the transmission spectrum and taking signal parametric measurements as required. It does not include acquisition of the information carried on the system. It is one of the techniques of COMSEC surveillance.

COMSEC software

Computer or microprocessor instructions and/or routines which control or perform COMSEC and COMSEC-related functions and associated documentation.

COMSEC surveillance

The systematic examination of telecommunications to determine the adequacy of COMSEC measures, to identify COMSEC deficiencies to provide data from which to predict the effectiveness of proposed COMSEC measures, and to confirm the adequacy of such measures after inplementation.

COMSEC survey

1. The application of COMSEC analysis and assessment techniques to a specific operation, function, or program.
2. Examination and inspection of a physical location to determine whether alterations and modifications are necessary to render it acceptable for the installation and operation of COMSEC equipment.

COMSEC system

The combination of all measures intended to provide communications security for a specific telecommunications system, including associated cryptographic, transmission, emission, computer and physical security measures, as well as the COMSEC support system (documentation; doctrine; keying material protection and distribution; and equipment engineering, production, distribution, modification, and maintenance).

contingency key	Keying material held for use on a cryptonet planned for establishment under specific operational conditions or in support of specific contingency plans.
controlled area	An area or space to which access is physically controlled.
controlled COMSEC item (CCI)	A marking applied to those unclassified end items and assemblies which perform critical COMSEC functions, and require access controls and physical security protection to assure their continued integrity.
controlling authority	The organization responsible for directing the establishment and operation of a cryptonet.
critical COMSEC function	A machine cryptosystem function which must be performed properly to prevent loss of COMSEC protection.
critical information	Information which must be protected to keep an adversary from gaining a significant military, political, or technical advantage.
cryptanalysis	The steps and operations performed in converting encrypted messages and plain text without initial knowledge of the key employed in the encryption. In COMSEC, its purpose is to evaluate the adequacy of the security protection that it is intended to provide, or to discover weaknesses or vulnerabilities which could be exploited to defeat, or lessen that protection.
*CRYPTO**	A marking or designator identifying all COMSEC keying material used to protect or authenticate telecommunications carrying national security and national security-related information.
crypto-alarm	A circuit or device in a crypto-equipment which detects failures or aberrations in the logic or operation of the crypto-equipment. It may inhibit transmission or may provide a visible or audible signal.
crypto-algorithm	A well-defined procedure or sequence of rules or steps which are used to produce cipher text from plain text and vice versa.

*1. The prefixes "crypt" and "crypto", in lower case, are abbreviations of "cryptographic" and are frequently combined with other terms to form compound words. When written in all upper case letters, "CRYPTO" has the specific meaning stated above.

2. Hyphenating "crypto": When the root word begins with a consonant, the form "crypto" is used and the combination is written as one word (cryptomaterial). When the root begins with a vowel, either "crypt" is used and the combination written as one word (cryptanalysis), or "crypto" is used and the combination is hyphenated (crypto-equipment).

crypto-ancillary equipment	1. Equipment designed specifically to facilitate efficient or reliable operation of crypto-equipment, but which does not perform cryptographic functions. 2. Equipment designed specifically to convert information to a form suitable for processing by crypto-equipment.
cryptodate	The date which determines the specific key to be employed.
crypto-equipment	Any equipment employing a cryptographic logic.
cryptographic	Pertaining to, or concerned with cryptography.
cryptographic logic	A deterministic logic by which information may be converted to unintelligible form and reconverted to intelligible form. (Sometimes referred to as "CRYPTOPRINCIPLE").
cryptography	1. The protection of telecommunications by rendering information unintelligible or unrecognizable until it reaches the intended recipient. 2. The design and use of cryptosystems.
cryptoguard	1. An activity responsible for decrypting, encrypting in another cryptosystem, and relaying telecommunications for other activities that do not hold compatible cryptosystems. 2. An activity responsible for providing secure telecommunications services for other activities.
crypto-ignition key (CIK)	A device or variable which splits or alters the cryptovariable so that a keyed crypto-equipment may be left unattended without being zeroized when the CIK is removed.
crypto-information	Information which would make a significant contribution to the cryptanalytic solution of encrypted text of a cryptosystem.
crypto-insecurity	An equipment malfunction or operator error which adversely affects the security of a cryptosystem.
cryptology	The science which deals with hidden, disguised, or encrypted communications. It embraces communications security and communications intelligence.

cryptomaterial	All material, including documents, devices, or equipment that contains crypto-information and is essential to the encryption, decryption, or authentiction of telecommunications.
cryptonet	Two or more activities which hold a short title (or MATSYM) of keying material in common.
cryptonet compartmentation	Limiting cryptonet size (i.e., the number of holders of a specific cryptovariable), as a means of controlling the volume of traffic protected by that cryptovariable or limiting the distribution of cryptovariables to specific user communities.
cryptonet controller	The operator of a communications terminal responsible for generating and distributing cryptovariables in electrical form.
cryptonet variable (CNV)	A cryptovariable held in common by all members of a secure communications net. This variable is usually used to secure all intra-net communications.
cryptoperiod	The time span during which a specific crytpovariable is authorized for use or in which the cryptovariables for a given system may remain in effect.
cryptoproduction equipment	Equipments, and components thereof, that are specifically designed for, and used in, the manufacture and associated testing of keying material in hard copy form.
cryptosecurity	The component of COMSEC which results from the provision of technically sound cryptosystems and their proper use.
cryptoservice message	A message, usually encrypted, transmitted between cryptocenters, requesting or supplying information regarding irregularities in encryption or decryption of messages.
cryptosystem	The associated items of COMSEC equipment or materials used as a unit to provide a single means of encryption or decryption.
cryptovariable	A sequence of random binary bits used to initially set up and periodically change permutations in a crypto-equipment for purposes of encrypting or decrypting electronic signals.

cryptovariable updating — A periodic cryptovariable modification performed automatically or manually to protect past traffic.

D

data encryption standard (DES) — An unclassified crypto-algorithm published by the National Bureau of Standards in FIPS PUB 46 for the protection of certain U.S. Government information.

decipher — To convert enciphered text to plain text by means of a cipher system.

decode — To convert encoded text into its equivalent plain text by means of a code.

decrypt — To convert encrypted text into its equivalent plain text by means of a cryptosystem. NOTE: The term decrypt encompasses the terms "decipher" and "decode".

DES device — The hardware part or subassembly which implements the DES algorithm.

DES equipment — An equipment embodying one or more DES devices and associated controls and power supplies used to implement the DES algorithm in a cryptosystem.

drop accountability — An accounting procedure by which a COMSEC account or subaccount receiving accountable COMSEC material assumes all responsibility after initial receipt and provides no further accounting to the central office of record.

dummy group — A group having the appearance of a valid code or cipher group but having no plaintext significance.

E

electronics security (ELSEC) — The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the interception and analysis of non-telecommunications electromagnetic, non-communications radiations, e.g., radar.

element — A subdivision of a COMSEC equipment, assembly or subassembly which normally consists of a single or group of replaceable parts. It is a removable item necessary to the operation of an equipment, but does not necessarily perform a complete function in itself.

emanations security — This term is no longer used. The definition of telecommunications has been expanded and emission security encompasses the old definition of emanations security.

emission security — That component of communications security (COMSEC) which results from all measures taken to deny unauthorized persons information of value which might be derived from intercept and analysis of compromising emanations from crypto-equipment and telecommunications systems.

encipher — To convert plain text into enciphered text by means of a cipher system.

encode — To convert plain text into encoded text by means of a code system.

encrypt — To convert plain text into unintelligible form by means of a cryptosystem. NOTE: The term encrypt encompasses the terms "encipher" and "encode".

end item — See COMSEC End Item

end item accounting — Accounting for all of the accountable components of a COMSEC equipment by a single short title.

end-to-end encryption — The protection of information passed in a secure telecommunications system by cryptographic means from point of origin to point of destination.

end-to-end security — The protection of information passed in a secure telecommunications system by cryptographic or protected distribution system means from point of origin to point of destination.

engineering development model — A model of COMSEC equipment to be used for engineering or operational tests under service conditions for evaluation or performance and military suitability.

exercise key — Cryptovariables intended for protection of on-the-air transmissions associated with field training or exercises.

exploratory development model (XDM) — An assembly of preliminary circuits or parts in line with commercial practices, to investigate, test, or evaluate the soundness of a concept, device, circuit, equipment or system in "breadboard" or rough experimental form without regard to eventual overall design form.

extraction resistance — The capability of a crypto-equipment to resist efforts to extract its cryptovariables.

F

fill device — An ancillary device used to transfer or store cryptovariables or to insert cryptovariables into a crypto-equipment; see "common fill devices"

fixed COMSEC facility — A facility which contains classified COMSEC material and is located in an immovable structure or on board a ship.

full maintenance — All diagnostic repair, modifications, and overhaul which are beyond the scope of limited maintenance. Depot maintenance shall include the repair of removable subassemblies, returned from limited maintenance, by piece part replacement.

G

global variable — A cryptovariable intended for emergency use by an entire communications net when the supporting key generation facility is unavailable or inoperable.

H

hand receipt — A document used to record local or temporary transfer of COMSEC material from a COMSEC custodian to a user.

high risk environment — A geographical area or specific location in which there are insufficient friendly security forces to ensure the safeguarding of installed machine cryptosystems.

hostile cognizant agent — A person who is authorized access to national security or national security-related information and who intentionally makes it available to an unauthorized party.

I

imitative communications deception — The introduction, by unauthorized parties, of signals or traffic which imitates valid messages into communications channels, to deceive authorized users.

initialization vector — A group of symbols used in defining the starting point of an encryption processs within a DES equipment.

integrated COMSEC equipment — Cryptographic equipment or circuitry which has been incorporated into another equipment whose primary function is not cryptographic.

intrusion detection system (IDS) — A system designed to detect and signal the entry of unauthorized persons into a protected area (e.g., security alarms, sensor systems, video systems).

inventory — 1. The physical verification of the presence of each item of accountable COMSEC material charged to a COMSEC account.
2. A listing of each item of accountable COMSEC material charged to a COMSEC account.

irregularly superseded keying material — Keying material used on an "as needed" basis, rather than during a specified period of time.

K

key — A sequence of symbols or their electrical or mechanical equivalents which, in machine or auto-manual crypto-systems, is combined with plain text to produce cipher text. (Often used informally as a synonym for keying material or cryptovariable).

key-auto-key — A cryptographic logic which uses previous key to produce key.

key card — A card containing a pattern of punched holes, which establishes the cryptovariable for a specific cryptonet at a specific time.

key cycle — A periodic sequence of key derived from a key generator in its successive states; one period is the key cycle and is usually marked by a return of the key generator to a former state.

key distribution center (KDC) — A COMSEC facility which generates and distributes cryptovariables in electrical form

key generator — A device or algorithm which employs a series of mathematical rules to deterministically produce a pseudo-random sequence of cryptovariables.

key list — A printed series of key settings for a specific cryptonet at a specified time, which is produced in list, padded, or tape form.

keystream — The sequence of key produced by a key generator.

key tape — A paper, mylar, or magnetic tape containing the key for a specific cryptonet at a specific time.

keying material — A type of COMSEC aid which supplies either encoding means for manual and auto-manual cryptosystems or cryptovariables for machine cryptosystems.

keying variables — See cryptovariable.

L

limited access area — An area containing classified information in which uncontrolled movement would allow access to classified information, but within which such access may be prevented by escort or other internal restrictions and controls.

limited maintenance — Maintenance performed by maintenance activities responsible for direct support of using organizations. Limited maintenance shall include disassembly, trouble isolation to a removable subassembly (i.e., printed circuit assembly, etc.), and replacement of the faulty subassembly without soldering. Limited maintenance will also provide technical assistance to using organizations.

limited protection — A form of short-term COMSEC protection applied to the electromagnetic or acoustic transmission of national security-related information.

limited protection equipment — An equipment which provides limited protection, e.g., VP–II equipment.

link encryption — The application of on-line cryptography to individual links of a communications system, so that all information passing over each link is encrypted in its entirety.

literal cryptosystem — A cryptosystem designed for literal communications, in which the plaintext elements are letters and sometimes the figures 0–9 or other symbols normally used in writing a language.

long title — The descriptive title of a TSEC–nomenclature item.

low probability of intercept (LPI) — A term describing signals that are difficult to detect, because their characteristics are hidden or disguised in some manner.

M

machine cryptosystem — A cryptosystem in which the cryptographic processes are performed by crypto-equipment.

maintenance key — Cryptovariables intended only for off-the-air, in-shop use.

manipulative communications deception — The alteration or simulation of friendly telecommunications for the purpose of deception.

manual cryptosystem — A cryptosystem in which the cryptographic processes are performed manually without the use of crypto-equipment, limited protection equipment, or auto-manual devices.

material symbol (MATSYM) — An unclassified identifier for certain key cards for resupply purposes.

message indicator — A group of symbols, usually placed at the beginning of the text of an encrypted message or transmission, which establishes the starting point of the key cycle.

mobile COMSEC facility — A facility which contains classified COMSEC material and is configured for operation while in motion.

modification — Any NSA-approved mechanical, electrical, or software change effecting the characteristics of a COMSEC end item. Classes of modifications are:
Mandatory Modification: A change which NSA requires be accomplished and reported by a specified Time Compliance Date. (NOTE: Should not be confused with a modification which NSA considers optional, but which has been adjudged mandatory by another Department/Agency/Service.)

Optional/Special Mission Modification: A change tailored to specific operational or environmental requirements, which NSA has determined does not require universal implementation.

Repair Action: An optional change provided for application by holders to enhance the operation, maintainability, or reliability of a COMSEC end item.

mythological designator — A name from mythology assigned for reference purposes to a particular cryptoprinciple and its associated crypto-equipment. (Mythological designators are no longer assigned for new systems.)

N

national COMSEC advisory memorandum (NACAM) — An NCSC document which provides advice and assistance to all departments and agencies of the Government on broad communications security matters consistent with the policy guidance of the Secretary of Defense and the Special Subcommitttee on Telecommunications protection. Such guidelines, approved by the Committee, are signed by the Chairman and issued by the Committee.

national COMSEC information memorandum (NACSIM) — An NCSC document which contains information of general interest or application pertaining to technical or procedural aspects of communications security. NACSIMs are published and disseminated by the Director, National Security Agency.

national COMSEC instruction (NACSI) — An NCSC document which provides instruction and establishes technical criteria to be implemented by the departments and agencies on specific communications security matters. NACSIs are promulgated by the Director, National Security Agency, after coordination with Committee members and other affected departments or agencies. NACSIs shall include legal guidelines, restrictions, and procedures promulgated by the Department of Defense and approved by the Attorney General that are generally applicable to the conduct of communications security activities.

national security information — Information related to the national defense or foreign relations of the United States that was determined to be classified pursuant to E.O. 12356 or any predecessor order.

national security-related information — Unclassified information related to the national defense or foreign relations of the United States.

no-lone zone — An area, room, or space to which no person may have unaccompanied access and which, when manned, must be occupied by two or more appropriately cleared individuals.

nonliteral cryptosystem — A cryptosystem intended for the transmission of data, in which the plaintext elements are signals or symbols other than the symbols normally used in writing a language.

null — A letter symbol or code group inserted in an encrypted message to delay or prevent its solution or to complete encrypted groups for transmission or transmission security purposes; a dummy letter.

O

off-line crypto-operation — Encryption or decryption performed separately and at a different time from the transmission or decryption, as by manual or machine crypto-equipments not electrically connected to a signal line.

one-part code — A code in which the plain text elements are arranged in alphabetical, numerical, or other systematic order accompanied by their code groups also arranged in alphabetical, numerical, or other systematic order, so that one listing serves for both encoding and decoding.

one-time cryptosystem — A cryptosystem employing keying variables which are only used once.

one-time pad — A manual, one-time cryptosystem produced in pad form.

one-time tape — A punched paper tape used on a one-time basis to provide cryptovariables in certain machine cryptosystems.

on-line crypto-operation — The use of crypto-equipment that is directly connected to a signal line, so that encryption and transmission are accomplished simultaneously.

operational key — Cryptovariables intended for use on-the-air for protection of mission-related, operational traffic.

operations code (OPCODE) — A code composed largely of words and phrases, which is capable of being used for general communications.

operations security (OPSEC) — The process of denying adversaries information about friendly capabilities and intentions by identifying, controlling, and protecting indicators associated with planning and conducting military operations and other activities.

OPSEC survey — A technique of data acquisition and analysis used to construct the sequence of events associated with time-definable operations and functions. It has as its objective the identification of activity which could be exploited by an adversary to gain a military, technical, diplomatic, or economic advantage and includes document reviews, interviews and observations, selective SIGSEC or COMSEC monitoring, and a review of all-source intelligence information bearing on adversary threats.

P

per-call variable — A cryptovariable which is generated on demand and distributed electrically to secure an individual period of intercommunication between members of a secure telecommunications network.

permuter — A device used in a crypto-equipment to change the order in which the contents of the shift register are used in various nonlinear combining circuits.

personnel insecurity — The capture, unauthorized absence, defection, or control by a hostile intelligence entity of an individual having knowledge of, or access to classified COMSEC information or material.

physical insecurity — Any occurrence (e.g., loss, theft, loss of control, capture, recovery by salvage, tampering, unauthorized viewing, access, or photographing) which results in jeopardy to COMSEC material.

physical security — The component of COMSEC which results from all physical measures necessary to safeguard COMSEC material and information from access thereto or observation thereof by unauthorized persons.

preproduction model — A model suitable for complete evaluation of mechanical and electrical form, design, and performance. It shall be in final mechanical and electrical form, employ standard parts, whenever possible, and be completely representative of the final equipment.

production model — A model in its final mechanical and electrical form of final production design made by production tools, jigs, fixtures, and methods using standard parts, whenever possible.

protected distribution system (PDS) — A wireline or fiber-optics system which includes adequate acoustical, electrical, electromagnetic, and physical safeguards to permit its use for the transmission of unencrypted classified information. NOTE: A complete PDS includes the subscriber and terminal equipment, as well as the interconnecting lines.

protective packaging — Packaging techniques for keying material which discourage penetration or which reveal that a penetration has occurred or which inhibit viewing or copying of keying material prior to the time it is exposed for use.

public cryptography — The body of cryptographic-related knowledge, study, techniques, and applications which is, or is intended to be, in the public domain.

public key cryptography — A type of cryptography in which the encryption process is publicly available and unprotected, but in which part of the decryption process is protected so that only a party with knowledge of both parts of the decryption process can decrypt the cipher text.

R

randomizer — A random bit generator which produces patterns used to modify the key variable of a crypto-equipment to establish a unique point on the key cycle at which encryption is to begin.

RED/BLACK concept — The concept that telecommunications circuits, components, equipments, and systems which handle classified plain-language information in electrical signal form (RED) be separated from those which handle encrypted or unclassified information (BLACK).

RED designation — A designation applied to telecommunications circuits, components, equipments, and systems which handle classified plain text or other information which requires protection during electrical transmission and to areas in which such information exists.

regionalization — A cryptovariable distribution concept whereby a group of subscribers in a secure telecommunications system assigned to a designated region or area are serviced by a particular key distribution center.

regularly superseded keying material — The keying material designated for use during a specific period of time, and superseded whether or not the key is used.

rekeying variable (RKV) — A cryptovariable used for encrypting other key variables when transmitting them electrically.

release — The authorized divulgence of U.S. cryptographic information or issuance of U.S. COMSEC material to foreign nations, international organizations, or U.S. contractors.

release prefix — A prefix used in the short titles of U.S.-produced keying material marked "CRYPTO" to indicate its foreign release status, "A" for material releasable to specific Allied nations, and "US" for material intended for exclusive U.S. use.

remote rekeying — The encrypted transmission of cryptographic key variables from a remote source.

reserve keying material — Uncommitted keying material held to satisfy unplanned keying material requirements.

risk — The probability that a hostile entity will successfully exploit a particular telecommunications or COMSEC system for intelligence purposes; its factors are threat and vulnerability.

S

sample key — Cryptovariables intended for demonstration use only.

SAVILLE advanced remote keying (SARK) — A keying technique used in certain cryptosystems, whereby keying variables are generated locally and distributed electrically.

secure subscriber facility — A secure telecommunications facility in which user-operated secure voice, data, facsimile, or video circuits terminate.

secure telecommunications facility — A telecommunications facility which employs crypto-material to protect the transmission of national security information.

seed variable — A cryptovariable which is initially loaded into a crypto-equipment and from which a sequence of updated variables is subsequently derived.

self-authentication — Implicit authentication of transmission on a secure telecommunications system or cryptonet to a predetermined classification level, through possession of the appropriate key.

sensitive compartmented information (SCI)	All information and material that requires special controls for restricted handling within compartmented intelligence systems and for which compartmentation is established.
shielded enclosure	An area (room or container) specifically designed to attenuate electromagnetic radiation or acoustic emanations, originating either inside or outside the area.
short title	An identifying combination of letters and numbers assigned to COMSEC material for brevity.
signals security (SIGSEC)	A generic term encompassing communications security and electronics security.
split knowledge	The separation of data into two or more parts, each part constantly kept under control of separate authorized individuals or teams, so that no one individual will be knowledgeable of the total data involved.
subassembly	A major subdivision of an assembly which consists of a package of parts, elements, and circuits which perform a specific function.
supersession	Scheduled or unscheduled replacement of a COMSEC aid with a different edition.
syllabary	In a code book, a list of individual letters, combination of letters, or syllables, accompanied by their equivalent code groups, to be used for spelling out words or proper names not present in the vocabulary of a code. Also known as spelling table.
synchronous crypto-operation	A method of on-line crypto-operation in which terminal crypto-equipments have timing systems to keep them in step.
system indicator	A symbol or group of symbols appearing in an encrypted message, which identifies the specific cryptosystems or keying material used in the encryption.

T

tampering — An unauthorized modification which alters the proper functioning of a COMSEC equipment or system in a manner which degrades the security it provides.

tape mixer — Teletypewriter security equipment which encrypts plain text and decrypts cipher text by combining them with data from a one-time tape.

telecommunications — The transmission, communication, or processing of information, including the preparation of such information therefor, by electrical, electromagnetic, electromechanical, or electro-optical means.

teleprocessing — The overall function of an information transmission system which combines telecommunications, automatic data processing, and man-machine interface equipment and their interaction as an integrated whole.

teleprocessing security — The protection resulting from all measures designed to prevent deliberate or inadvertent, unauthorized disclosure, acquisition, manipulation, or modification of information in a teleprocessing system.

TEMPEST — A short name referring to investigation and studies of compromising emanations. It is often used synonymously for the term "compromising emanations", e.g., TEMPEST tests, TEMPEST inspections.

test key — Cryptovariables intended for "on-the-air" testing of COMSEC or communications equipment or systems.

threat — The technical and operational capability of a hostile entity to detect, exploit, or subvert friendly telecommunications and the demonstrated, presumed, or inferred intent of that entity to conduct such activity.

time compliance date — The date by which a mandatory modification to a COMSEC end item must be incorporated, if the item is to remain approved for operational use.

traffic analysis — The study of communications characteristics which are external to the encrypted texts.

traffic-flow security — The capability of certain on-line, machine cryptosystems to conceal the presence of valid traffic.

training key — Cryptovariables intended for use on- or off-the-air in support of mission-related operational training.

TRANSEC variable — A cryptovariable employed for the purpose of maintaining transmission security.

transfer of accountability — The process of transferring the accountability of COMSEC material from the Central Office of Record of the shipping organizations, to the Central Office of Record of the receiving organization, or between commands or COMSEC custodians.

transmission security (TRANSEC) — The component of communications security which results from all measures designed to protect transmission from interception and exploitation by means other than cryptanalysis.

transportable COMSEC facility — A facility which contains classified COMSEC material and can readily be moved from one location to another, but is not configured for operation while in motion.

transmission authentication — A procedure whereby a station may establish the authenticity of its own transmission.

TSEC nomenclature — A system for identifying the type and purpose of items of COMSEC material over which NSA exercises configuration control. (NOTE: "TSEC" is an abbreviation for "telecommunications security".)

two-part code — A code consisting of two sections or parts, an encoding section in which the vocabulary items are arranged in alphabetical or other systematic order accompanied by their code equivalents arranged in nonalphabetical or random order, and a decoding section in which the code groups are arranged in alphabetical or numerical order and are accompanied by their plaintext meanings which are now in a mixed order.

two-person control — The close surveillance and control of certain COMSEC materials at all times by a minimum of two appropriately cleared and authorized persons, each capable of detecting incorrect and unauthorized procedures with respect to the tasks to be performed and each familiar with established security requirements.

U

unique variable (UV)

A rekeying variable held only by one crypto-equipment and its associated key distribution center.

user

An individual who is required to use COMSEC material in the performance of his official duties and who is responsible for its safeguarding.

V

variant

One of two or more code symbols which have the same plaintext equivalent.

vulnerability

Characteristics of a friendly telecommunications system or cryptosystem which are potentially exploitable by hostile intelligence entities.

vulnerability assessment

The systematic examination of telecommunications to determine the adequacy of COMSEC measures, to identify COMSEC deficiencies, to provide data from which to predict the effectiveness of proposed COMSEC measures, and to confirm the adequacy of such measures after implementation.

W

working variable

A cryptovariable distributed by a key generation facility for use on a specific inter-station call.

Z

Z variable

A cryptovariable used in certain cryptosystems to protect other variables contained in a key distribution data base.

zeroize

To remove or eliminate the cryptovariable from a crypto-equipment or fill device.

--- NOTES ---

--- NOTES ---

Approved For Release 2008/02/08 : CIA-RDP96M01138R000900020033-3